1. (**Currently Amended**) A method for generating an Identification and Verification Template (IVT) comprising the steps of:

obtaining a user biometric **from a biometric system, wherein, the user biometric includes previously encoded authorization information defining a set of privileges granted to a user by an authorization officer for a security infrastructure**; and

generating a ~~dependent~~ **dependency** vector from the user biometric, **wherein the dependency vector is generated with a lossy transformation of information stored in the user biometric;**

storing the dependency vector in an Identification and Verification Template (IVT) on a reliable storage medium, such that the ~~template~~ **IVT** is bound cryptographically to ~~the~~ **a** user **from which the user biometric was obtained, wherein the IVT does not include complete information from the obtained user biometric but does allow for verification of the user when the IVT is accessed for the security infrastructure at a later time**.

2. (**Currently Amended**) The method of claim 1, wherein the dependency vector includes check digits of the user biometric **generated** using an error correcting code.

3. **(Currently Amended)** The method of claim 1, wherein a canonical user biometric is generated from a **biometric processing** function of multiple readings of the ~~user's~~ **user** biometric from **the user**.

4. **(Currently Amended)** The method of claim 3, wherein the **biometric processing** function is a majority decoding function.

5. **(Currently Amended)** The method of claim 1, in which the ~~template~~ ~~contains~~ **IVT includes** public identification information **for the user**.

6. **(Currently Amended)** A method for uniquely identifying a user via biometric analysis comprising the steps of:

acquiring an input **from a user** comprising a User Biometric **(UB)** from ~~a~~ **an offline** reader ~~(UB)~~;

acquiring an input comprising an **Identification and Verification Template (IVT)** ~~IVT~~ from a token or card**, wherein the IVT was generated with a lossy transformation of a previously obtained UB, is cryptographically bound to a user from which the UB was obtained and wherein the IVT does not include complete information from the obtained UB but does allow for verification of the user when the IVT is accessed for a security infrastructure at a later**; and

performing a validation protocol ~~given as input~~ **with** the ~~user's biometric~~ **the** ~~(~~UB~~)~~ and the IVT, whereby a decision value is computed giving either ~~"AUTH"~~ **Authorization privileges** or ~~"Other",~~ **Other privileges to the user for access to th security infrastructure**, where "~~Other~~" **Other privileges** may be anything else but **Authorization privileges** ~~"AUTH",~~ **wherein the validation protocol does not require use of a compare operation between the acquired UB and the acquired IVT**.

7. (**Currently Amended**) The method of claim 6, ~~in which~~ **wherein** the validation protocol is a cryptographic validation mechanism for an authentication scheme.

8. (**Currently Amended**) The method of claim 6, ~~where~~ **wherein** the **acquired UB** ~~user biometric~~ is an iris scan or a portion of an iris scan **of the user**.

9. (**Currently Amended**) The method of claim 6, where the ~~user biometric (UB)~~ **acquired UB** is derived from a **biometric processing** function ~~of~~ **comprising** multiple scans of the ~~biometric~~ **UB**.

10. (**Currently Amended**) The method of claim 9, where the **biometric processing** function includes **a** ~~the use of~~ majority decoding **function**.

11. **(Currently Amended)** The ~~Method~~ **method** of claim 10, where the **biometric processing** function **further** includes error correction of **a** ~~the~~ biometric component after **the** majority decoding **function** is applied.

12. **(Currently Amended)** The method of claim 6, where the ~~biometric registration template~~ **IVT** incorporates a password encrypted value of the **IVT** ~~registration template~~.

13. **(Currently Amended)** A method of secure **biometric** pattern recognition ~~is provided~~ comprising the steps of:

acquiring a first **user biometric (UB)** pattern;

combining the **UB** pattern with authenticating information **with a lossy transformation of information stored in the UB**;

encrypting the combination of the **UB** pattern and the authenticating information to provide an **Identification and Verification Template (IVT)** ~~a template~~**, wherein the IVT includes less than all information obtained from the first UB**;

acquiring a second **UB** pattern; and

processing the second **UB** pattern and the **IVT** ~~template~~ to determine if the first **UB** pattern and the second **UB** pattern are the same.

14. **(Currently Amended)** ~~**A method of providing an individual verification template comprises the steps of: acquiring a biometric pattern from an individual; and**~~

~~**cryptographically combining the biometric pattern with authenticating information to provide the individual verification template**~~ **The method of Claim 13 wherein the processing step does not require use of a compare operation between the acquired second UB pattern and the IVT to securely identified a user associated with the second UB.**

15. **(New)** The method of claim 1, wherein the user biometric is an iris scan or a portion of an iris scan of the user.

16. **(New)** The method of claim 1, wherein the reliable storage medium includes a magnetic strip or smart card.